D21

N79-22161

Further Results on Fast Transforms for Decoding Reed-Solomon Codes Over $GF(2^n)$ for $n = 4,5,6,8$

I. S. Reed
Department of Electrical Engineering
University of Southern California

T. K. Truong, R. L. Miller, and B. Benjauthrit
Communications Systems Research Section

In this article it is shown that Winograd's methods can be modified to compute Fourier-like transforms over GF (2^n), where n = 4,5,6,8. Such transforms are used to encode and decode Reed-Solomon codes of block length 2^n-1. With these transforms a Reed-Solomon decoder can be made faster and more efficient than a decoder that uses the conventional fast transforms over GF(2^n).

I. Introduction

Fast transforms over the group $(Z_2)^n$ were used first by Green (Ref. 1) of the Jet Propulsion Laboratory to decode the (32,6) Reed-Muller code (Ref. 2) in the Mariner and Viking space probes. In 1971, Mandelbaum (Ref. 3) proposed to decode Reed-Solomon (RS) codes by a transform technique. Recently Gore (Ref. 4) extended Mandelbaum's method to decode RS codes with a finite field transform over $GF(2^n)$. Later, Michelson (Ref. 5) implemented Mandelbaum's algorithm and showed that a transform decoder over $GF(2^n)$ requires fewer multiplications than a more standard decoder (Refs. 6 and 7). The disadvantage of the transform method over $GF(2^n)$ is that the transform length is an odd number, so that the most efficient FFT algorithm cannot be used. Recently, the authors in (Ref. 8) showed that RS codes can be decoded with a combination of a fast transform and continued fractions. This approach was used to decode RS codes over $GF(2^{2^n})$ (Ref. 9), and over $GF(32)$ and $GF(64)$ (Ref. 10); Winograd's techniques were used to reduce the number of multiplications. In this paper we extend the results of Refs. 9 and 10 by providing a simple inspection technique to further cut down the number of multiplications.

Present plans for the space communication link for the Voyager mission (Ref. 11) include a 16-error-correcting, 255-symbol RS code, where each symbol has 8 bits. This RS code is concatenated with a Viterbi decoded convolutional code of constraint length 7, rate 1/2 or 1/3. Such a concatenated coding scheme can be used to reduce the signal-to-noise ratio required to meet a specified bit-error rate.

In order to decode a given received vector $r = (r_0, r_1, \ldots, r_{N-1})$ of such an RS code of length N by a transform technique, one first computes the syndromes (Ref. 8).

$$S_k = \sum_{i=0}^{N-1} r_i \gamma^{ki} = \sum_{i=0}^{N-1} (c_i + e_i) \gamma^{ki} = \sum_{i=0}^{N-1} e_i \gamma^{ki} = E_k$$

$$\text{for } k = 1,2, \ldots, 2t \tag{1}$$

where

t = maximum number of errors that can be corrected

$c = (c_0, c_1, \ldots, c_{N-1})$ = transmitted RS code word

$e = (e_0, e_1, \ldots, e_{N-1})$ = error pattern

and

$\gamma \epsilon\, GF(2^n)$ is a primitive Nth root of unity

The error locator polynomial is then determined from the syndromes and used to compute the remaining syndromes, $E_{2t+1}, \ldots, E_N = E_0$. The corrected RS code word is then $c = r - e$, where $e = (e_0, e_1, \ldots e_{N-1})$, the error word is the inverse transform of E_k given by the relation:

$$e_l = N^{-1} \sum_{k=0}^{N-1} E_k \gamma^{-lk}, \; l = 0, 1, \ldots, N-1 \tag{2}$$

Observe that (1) as well as its inverse (2) are actually discrete Fourier-like transforms of the form:

$$A_j = \sum_{i=0}^{N-1} a_i \gamma^{ij}, \; 0 \leqslant j \leqslant N-1, \; \gamma^N = 1 \tag{3}$$

Evidently, the computation of A_j in (3) directly involves N^2 multiplications. By appropriate algebraic manipulations, it is shown in this paper that this number of multiplications can be reduced substantially.

Eq. (3) can be rewritten in matrix form as

$$\begin{pmatrix} A_0 \\ A_1 \\ \\ . \\ . \\ . \\ A_{N-1} \end{pmatrix} = \begin{pmatrix} \gamma^{00} & \gamma^{01} & \ldots & \gamma^{0(N-1)} \\ \gamma^{10} & \gamma^{11} & \ldots & \gamma^{1(N-1)} \\ \gamma^{20} & \gamma^{21} & \ldots & \gamma^{2(N-1)} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ \gamma^{(N-1)0} & \gamma^{(N-1)1} & \ldots & \gamma^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \\ . \\ . \\ . \\ a_{(N-1)} \end{pmatrix} \tag{4}$$

or in abbreviated notation as

$$\bar{A} = W'\bar{a} \tag{5}$$

where W' is an $N \times N$ matrix (γ^{ij}), and $\bar{A}$ and $\bar{a}$ are $1 \times N$ column matrices (A_j) and (a_i), respectively. Also let

$$A_j = a_0 + B_j \quad \text{for } j = 1,2, \ldots, N-1$$

where

$$B_j = \sum_{i=1}^{N-1} a_i \gamma^{ij}$$

or again in a short notation as

$$\bar{B} = W\bar{a} \tag{6}$$

where W is the $(N-1) \times (N-1)$ matrix $(\gamma^{ij})_{i,j\neq 0}$ and $\bar{a}$, $\bar{B}$ are the column matrices (a_i) and (B_i), respectively. By factoring matrix W into a product of matrices $W = W_1 W_2 \ldots W_k$, Gentleman (Ref. 12) was able to reduce the number of multiplications involved in this computation considerably.

In this paper, algorithms using the methods of Winograd (Refs. 13 and 14) are developed to compute the above transform over $GF(2^n)$ for $n = 4,5,6,8$. The idea behind this method is to first permute the entries of the matrix W into a cyclic block of submatrices. Then, using some variations of the ideas of Winograd, the total number of multiplications required to perform the transform are significantly reduced. Two cases need to be distinguished.

First, if N is a prime number p, then there exists $\alpha \in GF(p)$, which generates the cyclic multiplicative group of $p-1$ elements. By applying the permutation $\sigma(i) = \alpha^i$, $i = 1, 2, \ldots, p-1$, the matrix W can be changed into a cyclic matrix $\widetilde{W}$ as follows:

$$B_{\sigma(j)} = \sum_{i=1}^{p-1} a_{\sigma(i)} \gamma^{\sigma(i)\sigma(j)} = \sum_{i=1}^{p-1} a_{\sigma(i)} \gamma^{\sigma(i+j)}, \; j = 1,2, \ldots, p$$

or

$$\widetilde{B} = \widetilde{W}\widetilde{a} \tag{7}$$

where $\widetilde{W} = (\gamma^{\sigma(i+j)})$ and where $a = (a_{\sigma(i)})$ and $B = (B_{\sigma(i)})$ are column matrices.

Secondly if N is not a prime, then it can be factored into a product of relatively prime powers $N = N_1 N_2 \ldots N_k$. Then by suitably applying the above technique for each N_i, the original $\bar{B}$ can be reconstituted by using the Chinese Remainder Theorem and Winograd's approach. The above proposed transform algorithm over $GF(2^n)$ generally requires fewer multiplications than the more conventional fast transform algorithm proposed by Gentleman (Ref. 12).

In the next section, methods for multiplying two polynomials by the cyclic convolution techniques are developed. Three examples, 3-, 5-, and 15-point cyclic convolutions, are provided to demonstrate the ideas involved. Section III contains technical results for simplifying computations over $GF(2^n)$. These results along with those in Section II about cyclic convolutions over $GF(2^n)$ are used to obtain the finite field transforms of 7 and 9 points in Section IV. Transforms of length $N = 3$, 5 and 17 points are given in Appendix B. In Section V finite field transforms of longer lengths, viz, $N = 2^n - 1$, where $n = 4,5,6,8$, are obtained, using the results given in Section III. A comparison of the new algorithm and Gentleman's algorithm is made in Section VI. Finally a comparison of the two algorithms in terms of the complexity of transform decoding of Reed-Solomon codes over $GF(2^n)$, $n = 4,5,6,8$ is provided in the last section of the paper.

II. Cyclic Convolutions Over $GF(2^n)$

The computation of transforms over $GF(2^n)$ will be based on fast cyclic convolutions. We first discuss a few techniques which are useful in obtaining fast cyclic convolutions.

Consider the multiplication of two polynomials $x(u) = x_0 + x_1 u^m$ and $y(u) = y_0 + y_1 u^m$ for $m = 1,2$ with coefficients in $GF(2^n)$. The product

$$\begin{aligned} x(u)y(u) &= (x_0 + x_1 u^m)(y_0 + y_1 u^m) \\ &= x_0 y_0 + [y_0(x_0 + x_1) + y_1(x_0 + x_1) + (x_0 y_0 + x_1 y_1)]\, u^m + x_1 y_1 u^{2m} \\ &= c_0 + c_1 u^m + c_2 u^{2m} \end{aligned} \tag{8}$$

where $c_0 = x_0 \cdot y_0$, $c_1 = (x_0 + x_1)(y_0 + y_1) + x_0 \cdot y_0 + x_1 \cdot y_1$ and $c_2 = x_1 \cdot y_1$. We see that only three multiplications are needed to perform (8), whereas a direct method would require four.

Now if $x(u) = x_0 + x_1 u + \ldots + x_{n-1} u^{n-1}$ and $y(u) = y_0 + y_1 u + \ldots + y_{n-1} u^{n-1}$ are two $(n-1)$th degree polynomials, then it is well known that the cyclic convolution $T(u)$ of the coefficients of $x(u)$ and $y(u)$ is given by the coefficients of

$$T(u) \equiv x(u)\, y(u) \bmod (u^n - 1) \tag{9}$$

The direct method for computing the above cyclic convolution $T(u)$ requires n^2 multiplications. This number of multiplications can be reduced by the first factoring $u^n - 1$ into distinct relatively prime factors

$$u^n - 1 = \prod_{i=1}^{k} m_i(u), \text{ when } n \text{ is odd} \tag{10}$$

Next compute the residues $T_i(u)$ of $T(u)$ as

$$T_i(u) \equiv T(u) \bmod m_i(u),\ i = 1,2,\ldots,k \tag{11}$$

Finally, $T(u)$ can be reconstructed from the residues $T_i(u)$ by the Chinese Remainder Theorem for polynomials (Ref. 15) as follows:

$$T(u) = T_1(u)M_1(u)M_1^{-1}(u) + \ldots + T_k(u)M_k(u)M_k^{-1}(u) \bmod (u^n - 1) \tag{12}$$

where

$$M_i(u)M_i^{-1}(u) = 1 \bmod m_i(u) \text{ for } i = 1,\ldots,k \tag{13}$$

Hence if the number of multiplications required to compute each $T_i(u)$ can be reduced, the total number of multiplications needed for $T(u)$ can also be reduced.

As an example, consider the cyclic convolution of 3 elements given in matrix form as

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_0 \\ a_2 & a_0 & a_1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \tag{14}$$

When it is clear it is convenient to let $[\ ]^C$ represent the cyclic convolution of a matrix of the type shown in (14). Also let $[\ ]^T$ denote the transpose of a matrix. Then (14) can be rewritten as:

$$[y_0, y_1, y_2]^T = [a_0, a_1, a_2]^C\ [x_0, x_1, x_2]^T \tag{15}$$

The above convolution is obtained from the coefficients of

$$T(u) = (a_2 + a_0u + a_1u^2) \cdot (x_2 + x_1u + x_0u^2) \bmod u^3 - 1 \tag{16}$$

Evidently a direct approach to compute (16) requires 9 multiplications. This number can be reduced to less than half as shown below.

To compute (16), factor $u^3 - 1 = (u - 1)(u^2 + u + 1) = m_1(u)m_2(u) = m_1(u)M_1(u) = m_2(u)M_2(u)$ where $m_1(a) = u - 1$ and $m_2(u) = u^2 + u + 1$. Here, the residues $T_i(u) \equiv T(u) \bmod m_i(u)$ are:

$$T_1(u) \equiv (a_2 + a_0 + a_1) \cdot (x_2 + x_1 + x_0) \bmod (u - 1)$$

and

$$T_2(u) \equiv [(a_2 + a_1) + (a_0 + a_1)u] \cdot [(x_2 + x_0) + (x_1 + x_0)u] \bmod (u^2 + u + 1)$$

Using the relations in (8), $T_2(u)$ is given by

$$T_2(u) \equiv (a_2 + a_1) \cdot (x_2 + x_0) + (a_0 + a_1) \cdot (x_1 + x_0) + [(a_2 + a_0)$$

$$\cdot (x_2 + x_1) + (a_2 + a_1) \cdot (x_2 + x_0)]\, u \bmod (u^2 + u + 1)$$

Evidently 3 multiplications are needed to compute $T_2(u)$. From the Chinese Remainder Theorem for polynomials (Ref. 15), $T(u)$ can be reconstructed from the residues $T_1(u)$ and $T_2(u)$ by the relation

$$T(u) \equiv T_1(u)M_1(u)M_1^{-1}(u) + T_2(u)M_2(u)M_2^{-1}(u) \bmod (u^3 - 1) \tag{17}$$

where $M_i^{-1}(u)$ uniquely satisfies the congruence $M_i(u)M_i^{-1}(u) \equiv 1 \bmod m_i(u)$ for $i = 1,2$. These equations are satisfied by $M_1^{-1}(u) = 1$ and $M_2^{-1}(u) = u$. Hence, from (17),

$$T(u) \equiv y_0 + y_1u + y_2u^2 \bmod (u^3 - 1) \tag{18}$$

where $y_0 = m_0 + m_1 + m_2$, $y_1 = m_0 + m_2 + m_3$, $y_2 = m_0 + m_3 + m_1$ and $m_0 = (a_2 + a_0 + a_1) \cdot (x_2 + x_1 + x_0)$, $m_1 = (a_2 + a_0) \cdot (x_2 + x_1)$, $m_2 = (a_2 + a_1) \cdot (x_2 + x_0)$, $m_3 = (a_0 + a_1) \cdot (x_1 + x_0)$. From (18), only four multiplications are needed to perform (15).

Next, consider the cyclic convolution of 5 elements of $GF(2^n)$. Again such a convolution is represented in matrix form as

$$[y_0, y_1, y_2, y_3, y_4]^T = [a_0, a_1, a_2, a_3, a_4]^C\ [x_0, x_1, x_2, x_3, x_4]^T \tag{19}$$

where $[\ ]^T$ and $[\ ]^C$ denote the transpose and the cyclic matrices, respectively, and $y_i, a_i, x_i \in GF(2^n)$ for $i = 0,1,2,3,4$. Again, this matrix equation can be obtained from the coefficients of

$$(a_4 + a_0u + a_1u^2 + a_2u^3 + a_3u^4) \cdot (x_4 + x_3u + x_2u^2 + x_1u^3 + x_0u^4) \bmod (u^5 - 1)$$

Since $u^5 - 1 = (u - 1)(u^4 + u^3 + u^2 + u + 1) = m_1(u)\,m_2(u) = m_1(u)\,M_1(u) = m_2(u)\,M_2(u)$, where $m_1(u) = u - 1$ and $m_2(u) = u^4 + u^3 + u^2 + u + 1$, the system of congruences $T_i(u) \equiv T(u) \bmod m_i(u)$ where $i = 1,2$ for this case is given by

$$T_1(u) \equiv (a_4 + a_0 + a_1 + a_2 + a_3) \cdot (x_4 + x_3 + x_2 + x_1 + x_0) \bmod (u - 1) \tag{20a}$$

and

$$\begin{aligned} T_2(u) \equiv\ & [(a_4 + a_3) + (a_0 + a_3)u + (a_1 + a_3)u^2 + (a_2 + a_3)u^3] \\ & \cdot [(x_4 + x_0) + (x_3 + x_0)u + (x_2 + x_0)u^2 \\ & + (x_1 + x_0)u^3] \bmod (u^4 + u^3 + u^2 + u + 1) \end{aligned} \tag{20b}$$

In order to compute (20b), let $c_0 = (a_4 + a_3)$, $c_1 = (a_0 + a_3)$, $c_2 = (a_1 + a_3)$, $c_3 = (a_2 + a_3)$, $d_0 = (x_4 + x_0)$, $d_1 = (x_3 + x_0)$, $d_2 = (x_2 + x_0)$, $d_3 = (x_0 + x_1)$. Then,

$$\begin{aligned} T_2(u) &\equiv [c_0 + c_1u + c_2u^2 + c_3u^3] \cdot [d_0 + d_1u + d_2u^2 + d_3u^3] \\ &\equiv [(c_0 + c_1u) + u^2(c_2 + c_3u)] \cdot [(d_0 + d_1u) + u^2(d_2 + d_3u)] \\ &\equiv [A_0 + A_1u^2] \cdot [B_0 + B_1u^2] \bmod (u^4 + u^3 + u^2 + u + 1) \end{aligned} \tag{21}$$

where $A_0 = c_0 + c_1u$, $A_1 = c_2 + c_3u$, $B_0 = d_0 + d_1u$ and $B_1 = d_2 + d_3u$. Now apply (8) at two levels, first to the expression $(A_0 + A_1u^2)(B_0 + B_1u^2)$ and second to the expression of the form $(A_0 + A_1) \cdot (B_0 + B_1) = [(c_0 + c_2) + (c_1 + c_3)u] \cdot [(d_0 + d_2) + (d_1 + d_3)u]$, etc. By this means one can show that the set of coefficients of $T_2(u)$ can be obtained with a total of only 9 multiplications. Finally, by the Chinese Remainder Theorem for polynomials (Ref. 15), $T(u)$ is given by

$$T(u) = y_0 + y_1u + y_2u^2 + y_3u^3 + y_4u^4 \tag{22}$$

where

$$\begin{aligned} y_0 &= m_0 + m_2 + m_9 + m_4 + m_5 + m_6, \\ y_1 &= m_0 + m_1 + m_9 + m_4 + m_5 + m_7, \\ y_2 &= m_0 + m_1 + m_9 + m_2 + m_5 + m_8, \\ y_3 &= m_0 + m_1 + m_6 + m_7 + m_2 + m_8 + m_9 + m_3 + m_4, \\ y_4 &= m_0 + m_1 + m_2 + m_3 + m_4 + m_5, \end{aligned}$$

and

$$m_0 = (a_0 + a_1 + a_2 + a_3 + a_4) \cdot (x_0 + x_1 + x_2 + x_3 + x_4),$$

$$m_1 = (a_0 + a_3) \cdot (x_3 + x_0),\ m_2 = (a_1 + a_3) \cdot (x_2 + x_0);$$

$$m_3 = (a_0 + a_2) \cdot (x_3 + x_1),\ m_4 = (a_2 + a_3) \cdot (x_1 + x_0);$$

$$m_5 = (a_4 + a_0 + a_2 + a_1) \cdot (x_4 + x_3 + x_2 + x_1);$$

$$m_6 = (a_1 + a_2) \cdot (x_2 + x_1),\ m_7 = (a_4 + a_0) \cdot (x_4 + x_3);$$

$$m_8 = (a_4 + a_1) \cdot (x_4 + x_2),\ m_9 = (a_4 + a_3) \cdot (x_4 + x_0).$$

Hence, by (22), the total number of multiplications required to perform (19) is 10.

We next consider the problem of computing the cyclic convolution of two sequences of l elements in $GF(2^n)$ when l is not a prime number. This requires a result of Winograd (Ref. 13).

Theorem 1: Let s and t be relatively prime positive integers and $A = (a_{ij})$ be the cyclic stXst matrix (defined in Appendix A). Then there exists a permutation π such that $B = (a_{\pi(i),\pi(j)})$ is partitioned into tXt submatrices, where each submatrix is cyclic and the submatrices themselves form an sXs cyclic matrix. For a proof see Ref. 14.

Now let $l = l_1 \cdot l_2 \ldots l_r$ where $(l_i, l_j) = 1$ for $i \neq j$. By repeated applications of Theorem 1, it is readily seen that if the number of multiplications used to compute the cyclic convolution of l_i points is m_i for $i = 1,2, \ldots, r$, then the number of multiplications needed to compute an l-point cyclic convolution is equal to $m_1, m_2, \ldots, m_r$.

Consider as an example the cyclic convolution of length 15 over $GF(2^n)$. By Theorem 1, one can permute the rows and columns of a 15X15 cyclic matrix in such a way that this matrix forms a 3X3 cyclic matrix with each matrix element being a 5X5 cyclic submatrix as follows:

$$[E_0, E_1, E_2]^T = [A, B, C]^C\ [Y_0, Y_1, Y_2]^T \tag{23}$$

where $E_0 = [y_0, y_6, y_{12}, y_3, y_9]^T$, $E_1 = [y_{10}, y_1, y_7, y_{13}, y_4]^T$, $E_3 = [y_5, y_{11}, y_2, y_8, y_{14}]^T$, $A = [a_0, a_6, a_{12}, a_3, a_9]^C$, $B = [a_{10}, a_1, a_7, a_{13}, a_4]^C$, $C = [a_5, a_{11}, a_2, a_8, a_{14}]^C$, and Y_i are the same as E_i with y_j replaced by x_j. By the same procedure used to compute the cyclic convolution of 3 elements, defined in (15), (23) becomes

$$E_0 = M_0 + M_1 + M_2,\ E_1 = M_0 + M_2 + M_3,\ E_2 = M_0 + M_3 + M_1 \tag{24}$$

where $M_0 = (A + B + C) \cdot (Y_0 + Y_1 + Y_2), M_1 = (C + A) \cdot (Y_1 + Y_2), M_2 = (C + B) \cdot (Y_2 + Y_0), M_3 = (A + B) \cdot (Y_0 + Y_1)$.

Clearly, (24) requires four (5X5) cyclic matrix multiplications. To find M_i for $i = 0,1,2,3$, one needs to multiply matrices of form $(A + B + C)$, $(C + A)$, $(C + B)$, and $(A + B)$ by vectors $(Y_0 + Y_1 + Y_2)$, $(Y_1 + Y_2)$, $(Y_2 + Y_0)$, and $(Y_0 + Y_1)$, respectively. Again, with the same procedure that was used to compute the cyclic convolutions of 5 elements given in (19), one finally obtains the number of multiplications needed to perform M_i for $i = 0,1,2,3$. Again each M_i can be obtained using 10 multiplications. Thus by (24) the total number of multiplications needed to compute the cyclic convolution of 15 elements in $GF(2^n)$ is 40.

Finally, consider the cyclic convolutions of two sequences, where the number of points is a power of 2. For example, con-

sider the cyclic convolution of two 4-element sequences over $GF(2^n)$. Such a convolution can be represented in matrix form as

$$[y_0, y_1, y_2, y_3]^T = [a_0, a_1, a_2, a_3]^C [x_0, x_1, x_2, x_3]^T \tag{25}$$

By Theorem 1 in Appendix A, (25) can be rewritten as

$$[Y_1, Y_2]^T = [A, B]^C [X_1, X_2]^T$$

where

$$Y_1 = [y_2, y_1]^T, \quad Y_2 = [y_2, y_3]^T, \quad X_1 = [x_0, x_1]^T, \quad X_2 = [x_2, x_3]^T,$$

$$A = \begin{bmatrix} a_0 & a_1 \\ a_1 & a_2 \end{bmatrix}$$

and

$$B = \begin{bmatrix} a_2 & a_3 \\ a_3 & a_0 \end{bmatrix}$$

According to (9), we have $Y_1 = D + E$ and $Y_2 = D + F$, where $D = A \cdot (X_1 + X_2)$, $E = (B - A) \cdot X_2$, and $F = (B - A) \cdot X_1$, so that three matrix multiplications are needed. Observe that D, E, and F are also 2-point transforms of the form

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b(x_1 + x_2) + (a + b)x_1 \\ b(x_1 + x_2) + (b + c)x_2 \end{pmatrix} \tag{26}$$

With the above decomposition, one may compute D, E, and F, each with 3 multiplications. Thus, the total number of multiplications needed to perform the cyclic convolution of 4 elements is 9.

III. The Computation of the Sum of Certain Elements of $GF(2^n)$ by Inspection

Sometimes, it is possible to show a priori that certain sums of elements of $GF(2^n)$ actually lie in the ground field $GF(2)$. That is, if s is such a sum, than $s = 0$ or $s = 1$. Hence multiplication by s need not be counted when considering the multiplicative complexity of an algorithm. This observation will be further studied in this section and utilized in the following sections. In this section, necessary and sufficient conditions are developed to determine when $s \epsilon GF(2^n)$ also lies in $GF(2)$. Moreover, if $s \epsilon GF(2)$, it is shown how to evaluate it by inspecting a certain polynomial. This method will be used to simplify the complexity of the transforms in the next section.

Theorem 2: Let $\alpha \epsilon GF(2^n)$ be a primitive $(2^n - 1)$th root of unity. Let

$$\beta = \sum_{i \epsilon I} \alpha^i$$

where $I \subseteq \{0,1,2, \ldots, 2^n - 1\}$. Then $\beta \epsilon GF(2)$ if and only if $2I = I$, where the multiplication by 2 is taken mod $(2^n - 1)$.

Proof: Let $\beta = \sum_{i \epsilon I} \alpha^i$. Then $\beta^2 = \left(\sum_{i \epsilon I} \alpha^i \right)^2 = \sum_{i \epsilon I} \alpha^{2i}$

Since $\beta \epsilon GF(2)$ iff $\beta^2 = \beta$, it follows that $\beta \epsilon GF(2)$ iff $\{2i \mid i \epsilon I\} = I$ or $2I = I$.

Example: Let $\alpha \epsilon GF(2^3)$ be a primitive 7th root of 1. Then $\alpha + \alpha^2 + \alpha^4 \epsilon GF(2)$ since the set $I = \{1;2,4\}$ is closed under multiplication by 2 (mod 7).

If $\beta \epsilon GF(2^n)$ satisfies the hypothesis of Theorem 2, one can determine whether $\beta = 0$ or $\beta = 1$. This will be indicated in Theorem 3. First, however, note that if $I \equiv \{0,1, \ldots, 2^n - 1\}$ has the property that $2I = I$, then one can express $I = I_1 \cup I_2 \cup \ldots \cup I_k$, as a disjoint union of sets such that

(i) $2I_j = I_j$ for $j = 1, \ldots, k$

and

(ii) I_j is minimal, i.e., if $I_j \supseteq I_{j'}$ and $2I_{j'} = I_{j'}$, then either $j = j'$ or $I_{j'} = \phi$.

In order to determine if

$$\beta = \sum_{i \epsilon I} \alpha^i = 0 \text{ or } 1$$

first reduce the problem to sets I_j satisfying (ii) as well as (i). Then by set union, one can determine the general case when $I = I_1 \cup \ldots \cup I_k$.

Lemma: Suppose $|I_j| = d_j$, where $|I_j|$ denotes the number of elements in set I_j and suppose that $2I_j = I_j$, then I_j is minimal if and only if

$$I_j = \left\{ i_0, 2i_0, \ldots, 2^{d_j - 1} i_0 \right\}$$

for any $i_0 \epsilon I_j$.

Proof: Suppose first that I_j is denoted as above. Since $2I_j = I_j$, it is clear that multiplication by 2 induces a cyclic permutation π on the elements $i_0, 2i_0, \ldots, 2^{d_j - 1} i_0$, with $\pi^{d_j}(i_0) = i_0$. Such a permutation is transitive; i.e., if $a, b \epsilon I_j$, then there exists an integer s, $0 \leqslant s < d_j$ such that $\pi^s(a) = b$. Thus it is clear that $I_j \neq I_k \cup I_l$ with $I_k \cap I_l = \phi$, $2I_k = I_k$, and $2I_l = I_l$. Conversely, suppose I_j is minimal, and let $i_0 \epsilon I_j$. Let s be the least positive integer such that $\pi^s(i_0) = i_0$. If $s < d_j$, then $\{i_0, 2i_0, \ldots, 2^{s-1} i_0\}$ is a proper subset of I_j closed under multiplication by 2. This contradicts the minimality of I_j. Thus $s = d_j$, hence

$$\left\{ i_0, 2i_0, \ldots, 2^{d_j - 1} i_0 \right\} = I_j$$

Theorem 3: Suppose $\beta \epsilon GF(2^n)$ and

$$\beta = \sum_{i \epsilon I_j} \alpha^i,$$

where $2I_j = I_j$ and I_j is minimal. Suppose also that $|I_j| = d_j$. Then α^{i_0}, where $i_0 \epsilon I_j$ satisfies some irreducible polynomial

$$p(x) = x^{d_j} + a_{d_j-1} x^{d_j-1} + \ldots + a_1 x + a_0$$

where $a_k \epsilon GF(2)$, and furthermore, $\beta = a_{d_j-1}$.

Proof: Let $i_0 \epsilon I_j$. Since I_j is minimal, it follows from the Lemma that

$$I_j = \left\{ i_0, 2i_0, \ldots, 2^{d_j-1} i_0 \right\}$$

Let

$$p(x) = x^m + a_{m-1} x^{m-1} + \ldots + a_i x + a_0$$

be the minimal polynomial of α^{i_0} over $GF(2)$. Then $p(\alpha^i) = 0$ for all $i \epsilon I_j$. Consequently, $m = \deg p(x) = d_j$ and

$$p(x) = \prod_{k=0}^{d_j-1} \left(x - \alpha^{i_0 2^k} \right)$$

By comparing the coefficients of x^{d_j-1} in $p(x)$ it is readily seen that

$$\beta = a_{d_j-1}$$

Example: Let $\alpha \epsilon GF(2^n)$ satisfy $x^3 + x^2 + 1 = 0$. Then $\alpha + \alpha^2 + \alpha^4 = 1$, the coefficient of x^2.

IV. A Modified Winograd's Algorithm for Computing a Transform Over $GF(2^n)$ of N Points for $N = 3,5,7,9,17$

In the introduction it was shown that a discrete Fourier transform defined in (3) can be appropriately rewritten via (5) and (6) in matrix form as shown in (7), namely, $\tilde{B} = \tilde{W}\tilde{a}$ where $\tilde{W}$ is an $(N-1) \times (N-1)$ cyclic matrix. In this section, these N-point transforms are performed by the cyclic convolution approach described in Section II for $N = 3,5,7,9,17$. These short-length transforms are used in the next section to compute transforms of longer lengths of $2^n - 1$ points, where $n = 4,5,6,8$. Only the cases for $N = 7$ and 9 are given explicitly in this section. The cases for $N = 3,5,17$ are given more briefly in Appendix B.

Consider first the case $N = 7$. Let γ be a primitive 7th root of unity in $GF(2^n)$. The transform over $GF(2^n)$ is expressible as

$$A_k = \sum_{i=0}^{7-1} a_i \gamma^{ik} \tag{27}$$

The permutation of σ for $N = 7$ is given by $\sigma(i) = 3^i \bmod 7$. Applying this permutation to (6) one obtains a 6X6 cyclic matrix equation. By Theorem 1 there exists a permutation π of rows and columns so that the 6X6 cyclic matrix can be partitioned into a 2X2 block matrix of 3X3 cyclic matrices. This is accomplished as follows:

$$[B_3, B_5, B_6, B_4, B_2, B_1]^T = [\gamma^2, \gamma^1, \gamma^4, \gamma^5, \gamma^6, \gamma^3]^C [a_3, a_5, a_6, a_4, a_2, a_1]^T$$

or

$$[E_1, E_2]^T = [A, B]^C [X_1, X_2]^T \tag{28}$$

where $E_1 = [B_3, B_5, B_6]$, $E_2 = [B_4, B_2, B_1]$, $A = [\gamma^2, \gamma^1, \gamma^4]^C$, $B = [\gamma^5, \gamma^6, \gamma^3]^C$, $X_1 = [a_3, a_5, a_6]^T$, $X_2 = [a_4, a_2, a_1]^T$. Using the 2-point cyclic convolution for the matrices in (28) yields

$$[E_1, E_2]^T = [D + E, D + F]^T$$

where $D = (X_1 + X_2) \cdot A$, $E = (B - A) \cdot X_2$, $F = (B - A) \cdot X_2$.

Since A and B are cyclic matrices, it is evident that the matrix $B - A$ is also a cyclic matrix. Using the same procedure for computing the 3-point cyclic convolution in (14) one can compute D, E, and F. Each of these quantities requires 4 multiplications. After some algebraic manipulations one finally arrives at the following expressions for the 7-point transform (27); namely,

$$\begin{aligned}
A_0 &= m_0, A_1 = m_0 + m_1 + m_2 + m_3 + m_4 + m_5 + m_6; \\
A_2 &= m_0 + m_1 + m_7 + m_2 + m_4 + m_8 + m_5; \\
A_3 &= m_0 + m_1 + m_3 + m_7 + m_9 + m_{10} + m_{11}; \\
A_4 &= m_0 + m_1 + m_3 + m_7 + m_4 + m_6 + m_8; \\
A_5 &= m_0 + m_1 + m_7 + m_2 + m_9 + m_{11} + m_{12}; \\
A_6 &= m_0 + m_1 + m_2 + m_3 + m_9 + m_{12} + m_{10}
\end{aligned} \tag{29}$$

where

$$m_0 = 1 \cdot (a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6);$$

$$m_1 = (\gamma^2 + \gamma^1 + \gamma^4 + 1) \cdot (a_3 + a_4 + a_5 + a_2 + a_6 + a_1);$$

$$m_2 = (\gamma^2 + \gamma^1) \cdot (a_5 + a_2 + a_3 + a_4);$$

$$m_3 = (\gamma^4 + \gamma^2) \cdot (a_6 + a_1 + a_5 + a_2);$$

$$m_4 = 1 \cdot (a_3 + a_3 + a_6);$$

$$m_5 = (\gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_5 + a_3);$$

$$m_6 = (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (a_6 + a_5);$$

$$m_7 = (\gamma^4 + \gamma^1) \cdot (a_6 + a_1 + a_3 + a_4);$$

$$m_8 = (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (a_6 + a_3);$$

$$m_9 = 1 \cdot (a_4 + a_2 + a_1);$$

$$m_{10} = (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (a_1 + a_2);$$

$$m_{11} = (\gamma^4 + \gamma^3 + \gamma^1 + \gamma^6) \cdot (a_1 + a_4);$$

$$m_{12} = (\gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_2 + a_4);$$

Now factor $x^7 - 1$ into a product of irreducible polynomials over $GF(2)$; i.e., $x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$. Let $I = \{2,1,4\}$. Then $2I = I$. By Theorem 2, $(\gamma^2 + \gamma^1 + \gamma^4) = 0$ or 1. Observe that I is minimal and $|I| = 3$. Next choose γ so that γ satisfies $x^3 + x^2 + 1$, then, by Theorem 3, $\gamma^2 + \gamma^1 + \gamma^4 = 1$. Thus m_1, in (29) is equal to zero. Hence, from (29), one observes that the number of multiplications needed to perform a 7-point transform over $GF(2^n)$ is 9, excluding the multiplications by the unit $\gamma^0 = 1$. In what follows it will be necessary to consider a multiplication by the element γ^0. Hence, if one includes multiplications by the unit $\gamma^0 = 1$, the number of multiplications needed to perform the above transform is 12.

Next consider $N_i = 3^2$. Let γ be the 9th root of unity in $GF(2^n)$. The permutation of W as defined in (6) for a 9-point transform over $GF(2^n)$ is given as follows:

$$\begin{pmatrix} b_2 \\ b_5 \\ b_8 \\ b_7 \\ b_4 \\ b_1 \\ b_3 \\ b_6 \end{pmatrix} = \begin{pmatrix} \gamma^4 & \gamma^8 & \gamma^7 & \gamma^5 & \gamma^1 & \gamma^2 & \gamma^3 & \gamma^6 \\ \gamma^8 & \gamma^7 & \gamma^5 & \gamma^1 & \gamma^2 & \gamma^4 & \gamma^6 & \gamma^3 \\ \gamma^7 & \gamma^5 & \gamma^1 & \gamma^2 & \gamma^4 & \gamma^8 & \gamma^3 & \gamma^6 \\ \gamma^5 & \gamma^1 & \gamma^2 & \gamma^4 & \gamma^8 & \gamma^7 & \gamma^6 & \gamma^3 \\ \gamma^1 & \gamma^2 & \gamma^4 & \gamma^8 & \gamma^7 & \gamma^5 & \gamma^3 & \gamma^6 \\ \gamma^2 & \gamma^4 & \gamma^8 & \gamma^7 & \gamma^5 & \gamma^1 & \gamma^6 & \gamma^3 \\ \gamma^3 & \gamma^6 & \gamma^3 & \gamma^6 & \gamma^3 & \gamma^6 & 1 & 1 \\ \gamma^6 & \gamma^3 & \gamma^6 & \gamma^3 & \gamma^6 & \gamma^3 & 1 & 1 \end{pmatrix} \begin{pmatrix} a_2 \\ a_5 \\ a_8 \\ a_7 \\ a_4 \\ a_1 \\ a_3 \\ a_6 \end{pmatrix} \tag{30}$$

The upper left 6×6 matrix of (30) is a cyclic matrix defined by

$$[Y_2, Y_5, Y_8, Y_7, Y_4, Y_1]^T = [\gamma^4, \gamma^1, \gamma^7, \gamma^5, \gamma^8, \gamma^2]^C \cdot [a_2, a_5, a_8, a_7, a_4, a_1]^T \tag{31}$$

By a procedure similar to that used to compute the matrix defined in (28), one obtains

$$Y_1 = m_1 + m_2 + m_3 + m_4 + m_5 + m_6,\ Y_4 = m_1 + m_7 + m_2 + m_4 + m_8 + m_5;$$

$$Y_2 = m_1 + m_3 + m_7 + m_9 + m_{10} + m_{11},\ Y_7 = m_1 + m_3 + m_7 + m_4 + m_6 + m_8;$$

$$Y_5 = m_1 + m_7 + m_9 + m_{11} + m_{12},\ Y_8 = m_1 + m_2 + m_3 + m_9 + m_{12} + m_{10}; \tag{32}$$

where

$$m_1 = (\gamma^4 + \gamma^1 + \gamma^7) \cdot (a_2 + a_7 + a_5 + a_4 + a_8 + a_1);$$

$$m_2 = (\gamma^4 + \gamma^1) \cdot (a_5 + a_4 + a_2 + a_7);$$

$$m_3 = (\gamma^7 + \gamma^4) \cdot (a_8 + a_1 + a_5 + a_4);$$

$$m_4 = (\gamma^4 + \gamma^1 + \gamma^7 + \gamma^5 + \gamma^8 + \gamma^2) \cdot (a_2 + a_5 + a_8);$$

$$m_5 = (\gamma^4 + \gamma^5 + \gamma^1 + \gamma^8) \cdot (a_5 + a_2);$$

$$m_6 = (\gamma^7 + \gamma^2 + \gamma^4 + \gamma^5) \cdot (a_8 + a_5);$$

$$m_7 = (\gamma^7 + \gamma^1) \cdot (a_8 + a_1 + a_2 + a_7);$$

$$m_8 = (\gamma^7 + \gamma^2 + \gamma^1 + \gamma^8) \cdot (a_8 + a_2);$$

$$m_9 = (\gamma^4 + \gamma^1 + \gamma^7 + \gamma^5 + \gamma^8 + \gamma^2) \cdot (a_7 + a_4 + a_1);$$

$$m_{10} = (\gamma^7 + \gamma^2 + \gamma^4 + \gamma^5) \cdot (a_1 + a_4);$$

$$m_{11} = (\gamma^7 + \gamma^2 + \gamma^1 + \gamma^8) \cdot (a_1 + a_7);$$

$$m_{12} = (\gamma^4 + \gamma^5 + \gamma^1 + \gamma^8) \cdot (a_4 + a_7).$$

If $x^9 - 1$ is factored into a product of irreducible polynomials over $GF(2)$, one has $x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$. Let $I = (4,1,7,5,8,2)$. Then $2I = I$. Observe that I is minimal and $|I| = 6$. For this case choose γ so that γ satisfies $x^6 + x^3 + 1$. Then, by Theorem 2 and Theorem 3 $(\gamma^4 + \gamma^1 + \gamma^7 + \gamma^5 + \gamma^8 + \gamma^2) = 0$ in (32). This implies $m_4 = m_9 = 0$ in (32). From (32), one observes that the number of multiplications needed to perform (31) is exactly 10.

The last two columns of the matrix defined in (30) can be obtained by the following 2X2 cyclic matrix

$$[x_1, x_2]^T = [\gamma^3, \gamma^6]^C [a_3, a_6]^T = [\gamma^3(a_3 + a_6) + (\gamma^3 + \gamma^6)a_6, \gamma^3(a_3 + a_6) + (\gamma^3 + \gamma^6)a_3]^T \tag{33}$$

But $\gamma^3 + \gamma^6 = 1$. Thus, (33) becomes

$$[x_1, x_2]^T = [\gamma^3(a_3 + a_6) + 1 \cdot a_6, \gamma^3(a_3 + a_6) + 1 \cdot a_1]$$

Similarly, the last two rows of the matrix defined in (30) can be obtained by computing the following cyclic matrix

$$[Z_1, Z_2]^T = [\gamma^3, \gamma^6]^C [a_1 + a_4 + a_7, a_2 + a_5 + a_8]^T$$

$$= [\gamma^3(a_1 + a_4 + a_7 + a_2 + a_5 + a_8) + 1 \cdot (a_2 + a_3 + a_8),$$

$$\gamma^3(a_1 + a_4 + a_7 + a_2 + a_5 + a_8) + 1 \cdot (a_1 + a_4 + a_7)]^T \tag{34}$$

Note that one multiplication is needed to compute (33). Similarly (34) requires only 1 multiplication. Thus, the algorithm for computing the 9-point transform is

$$b_0 = 1 \cdot (a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8);$$

$$b_1 = Y_1 + X_1 + 1 \cdot a_1, b_2 = Y_2 + X_2 + 1 \cdot a_0, b_3 = Z_1 + 1 \cdot (a_3 + a_6 + a_0);$$

$$b_4 = Y_4 + X_1 + 1 \cdot a_0, b_5 = Y_5 + X_2 + 1 \cdot a_0, b_6 = Z_1 + 1 \cdot (a_1 + a_6 + a_0);$$

$$b_7 = Y_7 + X_1 + 1 \cdot a_0, b_8 = Y_8 + X_2 + 1 \cdot a_0. \tag{35}$$

From (35), the total number of multiplications needed to perform a 9-point transform is 12, excluding multiplications by the unit 1. Again, the algorithms for computing N-point transforms over $GF(2^n)$ for $N = 3,5,17$ are given in Appendix B.

V. Transforms Over $GF(2^n)$ of 2^n-1 Points Where $n = 4,5,6,8$

For $N = N_1 N_2 \ldots N_k$, where $(N_i, N_j) = 1$, it was shown by Winograd in Refs. 13 and 14 that the transform matrix W' defined in (5) can be transformed into the product of $W'_1, W'_2, \ldots, W'_k$, where W'_i is the matrix of an N_i-point discrete Fourier-like transform. Assume that m_i multiplications are needed to perform an N_i-point transform over $GF(2^n)$ for $1 \leqslant i \leqslant k$. Then, $m_1 m_2 \ldots m_k$ multiplications are needed to compute the N-point transform.

Suppose $N = 2^4 - 1 = 3 \times 5$. Since the 15th roots of unity lie in $GF(2^4)$, $GF(2^4)$ is the appropriate domain for calculating the transform of 15 points using the algorithm described in the last paragraph of the previous section. The Chinese Remainder Theorem is used to represent each integer $i (0 \leqslant i < 15)$ by the pair $(i_1, i_2) = (i \bmod 3, i \bmod 5)$. Further, let γ_1, γ_2, and γ_3 be the 3rd, 5th and 15th roots of unity in $GF(2^4)$, respectively. Then, the 15-point transform over $GF(2^4)$ is

$$A_j = \sum_{i=0}^{14} a_i \gamma^{ij} \tag{36a}$$

After representing i and j by $i = (i_1, i_2) = (i \bmod 3, i \bmod 5)$ and $j = (j_1, j_2) = (j \bmod 3, j \bmod 5)$ respectively,

$$A_{(j_1, j_2)} = \sum_{i_1=0}^{2} \left[\sum_{i_2=0}^{4} a_{(i_1, i_2)} \gamma_2^{i_2 j_2} \right] \gamma_1^{i_1 \cdot j_1} = \sum_{k_1=0}^{2} a_{i_1}(j_2) \gamma_1^{i_1 \cdot j_1} \tag{36b}$$

where $a_{i_1}(j_2)$ is the 5-point transform over $GF(2^4)$ defined by

$$a_{i_1}(j_2) = \sum_{i_2=0}^{4} a_{(i_1, i_2)} \gamma_2^{i_2 \cdot j_2}$$

Expressing (36b) in matrix notation, we have

$$\left(a_{i_1}(j_2)\right) = W'_2 \bar{a}_{i_1}$$

where

$$W_2' = \begin{pmatrix} \gamma_2^0 & \gamma_2^0 & \gamma_2^0 & \gamma_2^0 & \gamma_2^0 \\ \gamma_2^0 & \gamma_2^1 & \gamma_2^2 & \gamma_2^3 & \gamma_2^4 \\ \gamma_2^0 & \gamma_2^2 & \gamma_2^4 & \gamma_2^1 & \gamma_2^3 \\ \gamma_2^0 & \gamma_2^3 & \gamma_2^1 & \gamma_2^4 & \gamma_2^2 \\ \gamma_2^0 & \gamma_2^4 & \gamma_2^3 & \gamma_2^2 & \gamma_2^1 \end{pmatrix}, \quad \bar{a}_{i_1} = \begin{pmatrix} a_{(i_1,0)} \\ a_{(i_1,1)} \\ a_{(i_1,2)} \\ a_{(i_1,3)} \\ a_{(i_1,4)} \end{pmatrix} \tag{37}$$

Thus (36) becomes

$$\bar{A}_{j_1} = \sum_{i_1=0}^{2} \gamma_1^{i_1 j_1} W_2' \bar{a}_{i_1} \quad \text{for } j = 0,1,2 \tag{38}$$

or

$$\begin{pmatrix} \bar{A}_0 \\ \bar{A}_1 \\ \bar{A}_2 \end{pmatrix} = \begin{pmatrix} W_2' & W_2' & W_2' \\ W_2' & W_2'\gamma_1 & W_2'\gamma_1^2 \\ W_2' & W_2'\gamma_1^2 & W_2'\gamma_1 \end{pmatrix} \begin{pmatrix} \bar{a}_0 \\ \bar{a}_1 \\ \bar{a}_2 \end{pmatrix}$$

where $\bar{A}_0$ is in terms of A_k as:

$$\bar{A}_0 = [A_{(0,0)}, A_{(0,1)}, A_{(0,2)}, A_{(0,3)}, A_{(0,4)}]^T = [A_0, A_6, A_{12}, A_3, A_9]^T \tag{39}$$

Similarly, $\bar{A}_1 = [A_{10}, A_1, A_7, A_{13}, A_4]^T$, $\bar{A}_2 = [A_5, A_{11}, A_2, A_8, A_{14}]^T$, and $\bar{a}_0$ through $\bar{a}_2$ are obtained from the expressions for $\bar{A}_0$ through $\bar{A}_2$ on replacing each A_i by a_i. Using the 3-point transform (B-1) in Appendix B and making the correspondence, $\gamma^0 \leftrightarrow W_2'$, $\gamma^1 \leftrightarrow W_2'\gamma_1$, $\gamma^2 \leftrightarrow W_2'\gamma_1^2$, one obtains

$$\bar{A}_0 = M_0 \;;\; \bar{A}_1 = M_0 + M_1 + M_2 \;;\; \bar{A}_2 = M_0 + M_1 + M_3 \tag{40}$$

where $M_0 = W_2'(\bar{a}_0 + \bar{a}_1 + \bar{a}_2)$, $M_1 = W_2'(\gamma_1 + 1)(\bar{a}_1 + \bar{a}_2)$, $M_2 = W_2'\bar{a}_2$, $M_3 = W_2'\bar{a}_1$. Thus, Eq. (40) requires four matrix multiplications.

Observe that all four matrix multiplications in (40) are 5-point transforms of exactly the same form as (B-2) in Appendix B. Thus one may compute M_j for $j = 0,1,2,3$ in (40) with a procedure similar to that used to compute the matrix defined in (B-2). The number of multiplications for computing an M_j for $j = 0,1,2,3$ in (40) is 5, excluding multiplication by γ^0. Thus, the total number of multiplications needed to compute a 15-point transform is $4 \times 5 = 20$.

Consider now a transform of $N = 31$ points. Let γ be a 31st root of unity in $GF(2^5)$. Here the 31×31 matrix is of the form given in (4) where $N = 31$. Now since $N = 31$ is prime, the permutation σ is given by $\sigma(i) = 3^i \bmod 31$, $i = 1,2,3,\ldots,30$. Using this permutation, one can permute the indices of B, a, W defined in (6) so that the matrix $\widetilde{W} = (\gamma^{\sigma(i)\sigma(j)})_{i,j\neq 0}$ is cyclic for $i,j = 1,2,\ldots,30$. Next since $N - 1 = 30 = 2 \times 15$, then, by Theorem 1, the 30×30 cyclic matrix $\widetilde{W}$ can be first partitioned into 15×15 submatrices where each submatrix is a 2×2 cyclic matrix. By (26), only three matrix multiplications are needed to

perform these 2 X 2 cyclic matrices. Also by (23), the number of multiplications needed to compute a 15 X 15 cyclic matrix is 40. Thus, the total number of multiplications needed to perform a 31-point transform is 3 X 40 = 120.

Next consider the finite field $GF(2^6)$. Since $N = 2^6 - 1 = 63 = N_1 \cdot N_2 = 7 \cdot 9$, by Winograd's algorithm one needs to compute an N_i-point transform over $GF(2^6)$ for $N_i = 7$ and 9. It was shown in the previous section that the number of multiplications needed to perform a 7-point transform over $GF(2^6)$ is 12, including the multiplications by the unit $\gamma^0 = 1$, and that the number of multiplications needed to perform a 9-point transform is 12, excluding multiplications by the unity $\gamma^0 = 1$. By the same procedure used to compute a 15-point transform over $GF(2^4)$ in (36a), the total number of multiplications needed to perform a 63-point transform over $GF(2^6)$ is 12 X 12 = 144.

Consider now the transform over $GF(2^8)$ of 255 points. Since $N = 255 = 3 \cdot 5 \cdot 17 = N_1 \cdot N_2 \cdot N_3$, by Winograd's algorithm one needs to compute an N_i-point transform over $GF(2^8)$ for $N_i = 3,5,17$. An N_i-transform over $GF(2^8)$ for $N_i = 3$, 5 and 17 is computed in Appendix B. With the procedure used to compute the 15-point transform over $GF(2^4)$ in (36a), the total number of multiplications needed to perform a 255-point transform over $GF(2^8)$ is 4 X 10 X 57 = 2180 multiplications.

VI. Comparison of New Algorithm With Gentleman's Algorithm

If $N = 2^n - 1 = N_1 \cdot N_2 \ldots N_k$, where $(N_i, N_j) = 1$ for $i \neq j$, Gentleman showed (Refs. 5 and 12) that an N-point transform N requires $N(N_1 + N_2 + \ldots + N_k - k + 1)$ multiplications. The present algorithm for computing the $(2^n - 1)$-point transform for $n = 4,5,6,8$ and Gentleman's algorithm are compared in Table 1. The number of multiplications needed to perform these algorithms is given in both cases. Evidently for $n = 4,5,6,8$ the new algorithm for computing the $(2^n - 1)$-point transform requires considerably fewer multiplications than Gentleman's algorithm.

VII. Transform Decoding of Reed-Solomon Codes

Let N be the block length of an RS code over $GF(2^n)$. Also let $d = 2t + 1$ be the minimum distance of the code, where t is the number of allowable errors. It was shown in Ref. 5 that a finite field transform over $GF(2^n)$ can be used to compute the syndrome and error magnitudes. It follows from Refs. 15 and 16 that the number of multiplications required to perform the syndrome and error magnitude calculations for the standard decoder is approximately $(N - 1)(d - 1) + t^2$.

For a $(2^n - 1, d)$ RS code where $d = 2t + 1$, the number of multiplications needed to compute the syndrome and the error magnitudes is given in Table 2 for $n = 4,5,6,8$. For comparison, the corresponding number of multiplications required by Gentleman's algorithm and by the standard algorithm are also given in the table.

Appendix A

Definition: An $n \times n$ matrix $A = (a_{ij})$ $(0 \leqslant i, j \leqslant n - 1)$ is cyclic if $a_{ij} = a_{i+1, j-1}$, where the indices are computed mod n.

Theorem 1: Let A by any $n \times n$ cyclic matrix, and suppose $n = a \times b$, where $(a, b) \neq 1$. Then A can be partitioned into a cyclic $a \times a$ matrix whose entries are themselves $b \times b$ submatrices.

Proof: Omitted.

Appendix B

This Appendix presents a brief summary of the transform algorithm of N points for $N = 3,5,17$. For $N = 3$, let γ be the 3rd root of unity in $GF(2^n)$ such that γ satisfies the irreducible polynomial $x^2 + x + 1$. The transform over $GF(2^n)$ is

$$A_k = \sum_{n=0}^{2} a_n \gamma^{nk} \quad \text{for } k = 0,1,2 \tag{B-1}$$

Let $m_0 = 1 \cdot (a_0 + a_1 + a_2)$, $m_1 = (a_1 + a_2) \cdot \gamma^1$, $m_2 = (\gamma^2 - \gamma^1) \cdot a_1 = 1 \cdot a_1$, and $m_3 = (\gamma^2 - \gamma^1) \cdot a_2 = 1 \cdot a_2$. Thus, $A_0 = m_0$, $A_1 = m_0 + m_1 + m_2$, and $A_2 = m_0 + m_1 + m_3$. Hence, the total number of multiplications needed to perform the above transform is 4, including multiplications by the unit 1.

Next consider the case $N = 5$. Let γ be a 5th root of unity in $GF(2^n)$ such that γ satisfies the irreducible polynomial $x^4 + x^3 + x^2 + x + 1$. The 5-point transform is

$$A_k = \sum_{n=0}^{5-1} a_n \gamma^{nk} \quad \text{for } k = 0,1,2,3,4 \tag{B-2}$$

Let $A_0 = \gamma^0 (a_0 + a_1 + a_2 + a_3 + a_4 + a_5)$, and also let $\sigma(i) = 2^i \bmod 5$. Equation (B-2) becomes

$$\tilde{B} = [B_2, B_4, B_3, B_1]^T = [\gamma^4, \gamma^3, \gamma^1, \gamma^2]^C [a_2, a_4, a_3, a_1]^T \tag{B-3}$$

By a procedure similar to that used to compute the cyclic convolution of 4 elements of $GF(2^n)$ in (25), one may compute (B-3). Thus, after some algebraic manipulations on (B-2) and (B-3) one arrives at the following expressions for the 5-point transform:

$$A_0 = m_0, A_1 = S_2 + m_5 + m_9, A_2 = S_1 + m_2 + m_6;$$

$$A_3 = S_1 + m_5 + m_8, A_4 = S_2 + m_4 + m_7. \tag{B-4}$$

where $m_0 = \gamma^0 \cdot (a_0 + a_1 + a_2 + a_3 + a_4)$, $m_1 = (\gamma^0 + \gamma^3) \cdot (a_1 + a_2 + a_3 + a_4)$, $m_2 = (\gamma^3 + \gamma^4) \cdot (a_2 + a_3)$, $m_3 = (\gamma^1 + \gamma^3) \cdot (a_1 + a_4)$, $m_4 = (\gamma + \gamma^4) \cdot (a_1 + a_3)$, $m_5 = (\gamma + \gamma^4) \cdot (a_2 + a_4)$, $m_6 = 1 \cdot a_1$, $m_7 = 1 \cdot a_3$, $m_8 = 1 \cdot a_4$, $m_9 = 1 \cdot a_2$, $S_1 = m_0 + m_1 + m_2$, $S_2 = m_0 + m_1 + m_3$.

If again one includes multiplications by the unit 1, it follows from the algorithm in (B-4) that the number of integer multiplications needed to perform a 5-point transform is 10. If multiplications by 1 are excluded, only 5 multiplications are needed.

Now consider the case $N = 17$. The permutation σ is $\sigma(i) = 5^i \bmod 17$. Applying this permutation to (6) one obtains a 16X16 cyclic matrix. By Theorem 2, the cyclic matrix can be partitioned into blocks of 4X4 matrices so that the blocks form a 4X4 cyclic matrix. This has the form

$$[T_2, T_4, T_3, T_1]^T = [A, B, C, D]^C [S_2, S_4, S_3, S_1]^T \tag{B-5}$$

where $T_2\ [b_5, b_8, b_6, b_{13}]^T, T_4 = [b_{14}, b_2, b_{10}, b_{16}]^T, T_3 = [b_{12}, b_9, b_{11}, b_4]^T, T_1 = [b_3, b_5, b_7, b_1]^T$.

$$A = \begin{pmatrix} \gamma^8, & \gamma^6, & \gamma^{14}, & \gamma^{13} \\ \gamma^6, & \gamma^{13}, & \gamma^{14}, & \gamma^2 \\ \gamma^{13}, & \gamma^{14}, & \gamma^2, & \gamma^{10} \\ \gamma^{14}, & \gamma^2, & \gamma^{10}, & \gamma^{16} \end{pmatrix}, \quad B = \begin{pmatrix} \gamma^2, & \gamma^{10}, & \gamma^{16}, & \gamma^{12} \\ \gamma^{10}, & \gamma^{16}, & \gamma^{12}, & \gamma^9 \\ \gamma^{16}, & \gamma^{12}, & \gamma^9, & \gamma^{11} \\ \gamma^{12}, & \gamma^9, & \gamma^{11}, & \gamma^4 \end{pmatrix}$$

$$C = \begin{pmatrix} \gamma^9, & \gamma^{11}, & \gamma^4, & \gamma^3 \\ \gamma^{11}, & \gamma^4, & \gamma^3, & \gamma^{15} \\ \gamma^4, & \gamma^3, & \gamma^{15}, & \gamma^7 \\ \gamma^3, & \gamma^{15}, & \gamma^7, & \gamma^1 \end{pmatrix}, \quad D = \begin{pmatrix} \gamma^{15}, & \gamma^7, & \gamma^1, & \gamma^5 \\ \gamma^7, & \gamma^1, & \gamma^5, & \gamma^8 \\ \gamma^1, & \gamma^5, & \gamma^8, & \gamma^6 \\ \gamma^5, & \gamma^8, & \gamma^6, & \gamma^{13} \end{pmatrix}$$

and S_1 through S_4 are obtained from the expressions for T_1 through T_4 on replacing each b_i by a_i.

By a procedure similar to that used to compute the cyclic matrix of 4 elements in (25), we obtain

$$\begin{aligned} T_2 &= V_1 + N_4 + N_6, \quad & T_4 &= V_2 + N_4 + N_7 \\ T_3 &= V_1 + N_5 + N_8, \quad & T_1 &= V_2 + N_5 + N_9 \end{aligned} \tag{B-6}$$

where

$$\begin{aligned} N_1 &= B(S_1 + S_2 + S_3 + S_4), \quad & N_2 &= (A + B) \cdot (S_2 + S_3), \\ N_3 &= (C + B) \cdot (S_1 + S_4), \quad & N_4 &= (C + A) \cdot (S_3 + S_1), \\ N_5 &= (C + A) \cdot (S_2 + S_4), \quad & N_6 &= E \cdot S_1 \\ N_7 &= E \cdot S_3, \ N_8 = E \cdot S_4, \quad & N_9 &= E \cdot S_2 \end{aligned} \tag{B-7}$$

and

$$V_1 = N_1 + N_2, \ V_2 = N_1 + N_3.$$

where $E = A + B + C + D$. Note that (B-7) requires nine (4X4) matrix multiplications. Observe that N_i for $i = 1,2, \ldots, 9$ in (B-6) can all be put in the form,

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} \gamma^1 & \gamma^2 & \gamma^3 & \gamma^4 \\ \gamma^2 & \gamma^3 & \gamma^4 & \gamma^5 \\ \gamma^3 & \gamma^4 & \gamma^5 & \gamma^6 \\ \gamma^4 & \gamma^5 & \gamma^6 & \gamma^7 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} \tag{B-8}$$

To compute (B-8), write it as

$$\begin{pmatrix} F_0 \\ F_1 \end{pmatrix} = \begin{pmatrix} J & K \\ K & L \end{pmatrix} \begin{pmatrix} E_0 \\ E_1 \end{pmatrix} = \begin{pmatrix} U_1 + U_2 \\ U_1 + U_3 \end{pmatrix} \tag{B-9}$$

where $U_1 = (E_0 + E_1) \cdot K$, $U_2 = (J + K) \cdot E_0$, $U_3 = (L + K) \cdot E_0$ are three (2X2) matrix multiplications.

The matrix U_1 in (B-9) is given by the relationship

$$U_1 = \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} = \begin{pmatrix} \gamma^3 & \gamma^4 \\ \gamma^4 & \gamma^5 \end{pmatrix} \begin{pmatrix} a_1 + a_3 \\ A_2 + a_4 \end{pmatrix}$$

$$= \begin{pmatrix} (a_1 + a_3 + a_2 + a_4) \cdot \gamma^4 + (\gamma^3 + \gamma^4) \cdot (a_1 + a_3) \\ (a_1 + a_3 + a_2 + a_4) \cdot \gamma^4 + (\gamma^4 + \gamma^5) \cdot (a_1 + a_3) \end{pmatrix}$$

The matrices U_2 and U_3 in (B-9) can also be obtained in a similar manner.

Now, let

$$\begin{aligned} M_1 &= \gamma^4 \cdot (a_1 + a_2 + a_3 + a_4), & M_2 &= (a_1 + a_3) \cdot (\gamma^3 + \gamma^4); \\ M_3 &= (\gamma^4 + \gamma^5) \cdot (a_1 + a_3), & M_4 &= (\gamma^2 + \gamma^4) \cdot (a_1 + a_2); \\ M_5 &= (\gamma^4 + \gamma^6) \cdot (a_1 + a_2), & M_6 &= (\gamma^1 + \gamma^3 + \gamma^2 + \gamma^4) \cdot a_1; \\ M_7 &= (\gamma^2 + \gamma^4 + \gamma^3 + \gamma^5) \cdot a_1, & M_8 &= (\gamma^3 + \gamma^5 + \gamma^4 + \gamma^6) \cdot a_1; \\ M_9 &= (\gamma^4 + \gamma^6 + \gamma^5 + \gamma^7) \cdot a_1. \end{aligned} \tag{B-10}$$

Thus,

$$\begin{aligned} b_1 &= M_1 + M_2 + M_4 + M_6, & b_2 &= M_1 + M_3 + M_4 + M_7; \\ b_3 &= M_1 + M_2 + M_5 + M_8, & b_4 &= M_1 + M_3 + M_5 + M_9 \end{aligned} \tag{B-11}$$

From (B-11), the total number of multiplications needed to perform (B-8) is 9.

To compute N_i for i = 1,2,3,4,5, defined in (B-7), the same procedure can be used that was used above for (B-8). The number of multiplications for comparing each of these M_j's is 9. To compute N_i for i = 6,7,8,9, for example, consider $N_6 = E \cdot S_1$,

$$N_6 = \begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \end{pmatrix} = \begin{pmatrix} \gamma^8+\gamma^2+\gamma^9+\gamma^{15}, \gamma^6+\gamma^{10}+\gamma^{11}+\gamma^7, \gamma^{13}+\gamma^{16}+\gamma^4+\gamma^1, \gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5 \\ \gamma^6+\gamma^{10}+\gamma^{11}+\gamma^7, \gamma^{13}+\gamma^{16}+\gamma^4+\gamma^1, \gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5, \gamma^2+\gamma^9+\gamma^{15}+\gamma^8 \\ \gamma^{13}+\gamma^{16}+\gamma^4+\gamma^1, \gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5, \gamma^2+\gamma^9+\gamma^{15}+\gamma^8, \gamma^{10}+\gamma^{11}+\gamma^7+\gamma^6 \\ \gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5, \gamma^2+\gamma^9+\gamma^{15}+\gamma^8, \gamma^{10}+\gamma^{11}+\gamma^7+\gamma^6, \gamma^{16}+\gamma^4+\gamma^1+\gamma^{13} \end{pmatrix} \begin{pmatrix} a_3 \\ a_{15} \\ a_7 \\ a_1 \end{pmatrix} \quad \text{(B-12)}$$

By a procedure similar to that used to compute the cyclic matrix defined in (B-8), one obtains

$$M_1 = (\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5)\cdot(a_3+a_{15}+a_7+a_1);$$

$$M_2 = (\gamma^{13}+\gamma^{16}+\gamma^4+\gamma^1+\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5)\cdot(a_3+a_7);$$

$$M_3 = (\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5+\gamma^2+\gamma^9+\gamma^{15}+\gamma^8)\cdot(a_3+a_7);$$

$$M_4 = (\gamma^6+\gamma^{10}+\gamma^{11}+\gamma^7+\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5)\cdot(a_3+a_{15});$$

$$M_5 = (\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5+\gamma^{10}+\gamma^{11}+\gamma^7+\gamma^6)\cdot(a_3+a_{15});$$

$$M_6 = (\gamma^8+\gamma^2+\gamma^9+\gamma^{15}+\gamma^6+\gamma^{10}+\gamma^{11}+\gamma^7+\gamma^{13}+\gamma^{16}+\gamma^4+\gamma^1+\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5)\cdot a_3;$$

$$M_7 = (\gamma^6+\gamma^{10}+\gamma^{11}+\gamma^7+\gamma^{13}+\gamma^{16}+\gamma^4+\gamma^1+\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^{15}+\gamma^2+\gamma^9+\gamma^{15}+\gamma^8)\cdot a_3;$$

$$M_8 = (\gamma^{13}+\gamma^{16}+\gamma^4+\gamma^1+\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5+\gamma^2+\gamma^9+\gamma^{15}+\gamma^8+\gamma^{10}+\gamma^{11}+\gamma^7+\gamma^6)\cdot a_3;$$

$$M_9 = (\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5+\gamma^2+\gamma^9+\gamma^{15}+\gamma^8+\gamma^{10}+\gamma^{11}+\gamma^7+\gamma^6+\gamma^{16}+\gamma^4+\gamma^1+\gamma^{13})\cdot a_3;$$

and

$$n_1 = M_1+M_2+M_4+M_6, \quad n_2 = M_1+M_3+M_4+M_7;$$

$$n_3 = M_1+M_2+M_5+M_8, \quad n_4 = M_1+M_3+M_5+M_9$$

Now, factor $x^{17}-1$ into a product of irreducible polynomials, i.e., $x^{17}-1 = (x-1).(x^8+x^7+x^6+x^4+x^2+x+1)\cdot(x^8+x^5+x^4+x^3+1)$. If one chooses γ such that γ satisfies $x^8+x^7+x^6+x^4+x^2+x+1$, then, by Theorem 2 and Theorem 3, $\gamma^6+\gamma^{10}+\gamma^{11}+\gamma^7+\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5$ and $\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5+\gamma^{10}+\gamma^{11}+\gamma^7+\gamma^6$ are equal to zero and $\gamma^6+\gamma^{10}+\gamma^{11}+\gamma^7+\gamma^{15}+\gamma^{16}+\gamma^4+\gamma^1+\gamma^{14}+\gamma^{12}+\gamma^3+\gamma^5+\gamma^2+\gamma^9+\gamma^{15}+\gamma^8=1$. These identities are used to reduce the M_k's; e.g., $M_4 = 0$, etc. After this reduction it can be shown that the total number of multiplications needed to perform (B-12) is 7, including multiplications by γ^0. If multiplications by γ^0 are excluded, evidently only 3 multiplications are actually needed. In a similar fashion, matrices N_7, N_8, and N_9 in (B-7) can be computed. After combining the above results, it is seen that the total number of multiplications needed to perform a 17-point transform over $GF(2^n)$ is $5 \times 9 + 4 \times 3 = 57$, excluding multiplications by γ^0. To include multiplications by γ^0, the total number of multiplications is $5 \times 9 + 4 \times 7 + 1 = 74$.

Acknowledgment

The authors wish to thank Dr. S. A. Butman, Manager of Communications Systems Research Section and Dr. N. A. Renzetti, Manager of Tracking and Data Acquisition Engineering, Jet Propulsion Laboratory, for their encouragement of the research which led to this paper.

References

1. Green, R. R., "Analysis of a Serial Orthogonal Decoder," *Space Programs Summary 37-53*, Vol. III, pp. 185–187, Jet Propulsion Laboratory, Pasadena, Calif., 1968.
2. Reed, I. S., "A Class of Multiple-Error-Correcting Codes and the Decoding Scheme," *IRE Trans.*, PGIT-4, 1954, pp. 38–49.
3. Mandelbaum, D., "On Decoding Reed-Solomon Codes," *IEEE Trans. Inform. Theory*, Vol. IT-17, No. 6, pp. 707–712, Nov. 1971.
4. Gore, W. C., "Transmitting Binary Symbols with Reed-Solomon Code," Johns Hopkins EE Report No. 73-5, Apr. 1973.
5. Michelson, A., "A New Decoder for the Reed-Solomon Codes Using a Fast Transform Technique," Systems Engineering Technical Memorandum No. 52, Electronic Systems Group, Eastern Division, GTE Sylvania, Aug. 1975.
6. Peterson, W. W., *Error-Correcting Codes*, MIT Press, Cambridge, Mass., pp. 168–169, 1961.
7. Lin, S., *An Introduction to Error-Correcting Codes*, Prentice-Hall, Englewood Cliffs, N.J., 1970.
8. Reed, I. S., Scholtz, R. A., Truong, T. K., and Welch, L. R., "The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms and Continued Fractions," *IEEE Trans. Inform. Theory*, Vol. IT-24, No. 1, pp. 100–106, Jan. 1978.
9. Reed, I. S., Truong, T. K., and Benjauthrit, B., "Transform Decoding of Reed-Solomon Codes over $GF(2^{2^n})$ Using the Techniques of Winograd," in *The Deep Space Network Progress Report 42-43*, pp. 141–163, Jet Propulsion Laboratory, Pasadena, Calif., Feb. 15, 1978.
10. Reed, I. S., Truong, T. K., and Benjauthrit, B., "On Decoding of Reed-Solomon Codes over $GF(32)$ and $GF(64)$ Using the Transform Techniques of Winograd," in *The Deep Space Network Progress Report 42-44*, pp. 139–171, Jet Propulsion Laboratory, Pasadena, Calif., Apr. 15, 1978.
11. Odenwalder, J., et al., "Hybrid Coding Systems Study Final Report," Linkabit Corp., NASA CR 114, 486, Sept. 1972.
12. Gentleman, W. M., "Matrix Multiplication and Fast Fourier Transforms," *Bell System Technical Journal*, 1968, pp. 1099–1103.
13. Winograd, S., "On Computing the Discrete Fourier Transform," *Proc. Nat. Acad. Sci. USA*, 1976, 73, pp. 1005–1006.

14. Winograd, S., "On Computing the Discrete Fourier Transform," Research Report, Math. Science Dept., IBM Thomas J. Watson Research Center, Yorktown Heights, New York, 10592.

15. Berlekamp, E. R., *Algebraic Coding Theory*, New York, McGraw Hill, 1968.

16. Forney, G. D., "On Decoding BCH Codes," *IEEE Trans. Inform. Theory*, Vol. IT-11, Oct. 1965.

Table 1. The complexity of transform over $GF(2^n)$ for $n = 4,5,6,8$

$N = 2^n - 1$	Factors $N_1 \cdot N_2 \cdots N_k$	No. Mult. of New Algorithm	No. Mult. of Gentleman's Algorithm $N(N_1 + N_2 + \ldots + N_k - k + 1)$
$2^4 - 1$	3×5	$4 \times 5 = 20$	$15(3 + 5 - 1) = 105$
$2^5 - 1$	31	120	961
$2^6 - 1$	7×9	$12 \times 12 = 144$	$63(7 + 9 - 1) = 945$
$2^8 - 1$	$3 \times 5 \times 17$	$4 \times 10 \times 57 = 2280$	$255(3 + 5 + 17 - 2) = 5865$

Table 2. The complexity of decoding RS of 2^n-1 points for $n = 4,5,6,8$

N	Factors $N_1, N_2, \ldots, N_k$	No. Mult. of New Algorithm	No. Mult. of Gentleman's Algorithm $2N(N_1 + N_2 + \ldots + N_k - k + 1)$	No. Mult. of Standard Algorithm $(N - 1)(d - 1) + t^2$
15	3×5	$2 \times 20 = 40$	$2 \times 105 = 210$	$14 \times 8 + 4^2 = 128$
31	31	$2 \times 120 = 240$	$2 \times 961 = 1922$	$30 \times 16 + 8^2 = 544$
63	7×9	$2 \times 132 = 264$	$2 \times 945 = 1890$	$62 \times 30 + 15^2 = 2085$
255	$3 \times 5 \times 17$	$2 \times 2280 = 4560$	$2 \times 5862 = 11724$	$254 \times 32 + 16^2 = 8384$